Data protection self assessment report

At a glance (overall rating)

Data protection assurance

Overall rating: green

0: Measures not implemented/planned
0: Measures partially implemented/planned
10: Measures successfully implemented

Records management

Overall rating: green

0: Measures not implemented/planned
1: Measures partially implemented/planned
13: Measures successfully implemented

Information security

Overall rating: green

0: Measures not implemented/planned
0: Measures partially implemented/planned
19: Measures successfully implemented

Data sharing & subject access

Overall rating: green

0: Measures not implemented/planned
0: Measures partially implemented/planned
9: Measures successfully implemented

Your business has established an appropriate data protection policy.

Successfully implemented

Your business has nominated a data protection lead.

Successfully implemented

Your business provides data protection awareness training for all staff.

Successfully implemented

Your business has registered with the Information Commissioner's Office.

Successfully implemented

Your business has made privacy notices readily available to individuals.

Successfully implemented

Your business has established a process to recognise and respond to individuals' requests to access their personal data.

Successfully implemented

Your business has established processes to ensure personal data is of sufficient quality to make decisions about individuals.

Successfully implemented

Your business has established a process to routinely dispose of personal data that is no longer required in line with agreed timescales.

Successfully implemented

Your business has established an information security policy supported by appropriate security measures.

Successfully implemented

Your business has established a process to ensure new projects or initiatives are privacy-proofed at the planning stage.

Successfully implemented

Your business carries out periodic checks on records security and there is monitoring of compliance with records management procedures. The outcomes of any records security checks or compliance monitoring is measured against key performance indicators to provide strategic oversight to those with overall responsibility for RM.

Partially implemented/planned

You business has defined and allocated records management responsibilities.

Successfully implemented

Your business has approved and published an appropriate records management policy. This is subject to a regular review process.

Successfully implemented

Your business has identified records management risks as part of a wider information risk management process.

Successfully implemented

Your business incorporates records management (RM) within a formal training programme. This comprises mandatory RM induction training with regular refresher material, and specialist training for those with specific RM functions.

Successfully implemented

Your business has minimum standards for creation of paper or electronic records and has established processes to ensure that there is a legitimate purpose for using personal data prior to collecting it.

Successfully implemented

Your business has identified manual and electronic records keeping systems throughout the organisation and a centralised record of those systems is actively maintained.

Successfully implemented

Your business has processes in place to ensure that personal data that is collected is accurate, adequate, relevant and not excessive. Routine weeding is also carried out to remove any personal data or records that are no longer relevant or out of date.

Successfully implemented

Your business has appropriate measures in place for the transfer of electronic records off-site to protect personal data from loss of theft.

Successfully implemented

Your business stores paper and electronic records securely with appropriate environmental controls and higher levels of security around sensitive personal data.

Successfully implemented

Your business restricts access to records storage areas in order to prevent unauthorised access, damage, theft or loss. Access should be role based in line with the principle of least privilege and checked regularly.

Successfully implemented

Your business has a process to assign user accounts to authorised individuals and to remove them when no longer appropriate. Such access should be granted on the basis of least privilege and have appropriate access controls in place.

Successfully implemented

Your business has business continuity plans in place. These should identify business critical records that are essential to the continued functioning or reconstitution of the organisation in the event of a disaster. Data that is stored electronically should be routinely backed-up to help restore information in the event of disaster.

Successfully implemented

Your business has a retention and disposal schedule in place which details how long manual and electronic records will be kept for.

Your business has defined confidential waste disposal processes in place to ensure that records are destroyed to an appropriate standard once a disposal decision has been made.

Successfully implemented

Your business has established a process to identify, assess and manage information security risks.

Your business ensures information security risks are assessed and appropriately managed.

Successfully implemented

Senior management has approved and published an appropriate information security policy.

Your business provides management direction and support for information security in accordance with business needs and relevant laws and regulations.

Successfully implemented

Your business has defined and allocated information security responsibilities.

Your business has established a management framework to coordinate and review the implementation of information security.

Successfully implemented

Your business has established written agreements with third party service providers that include appropriate information security conditions.

Your business ensures the protection of personal data that is accessed by suppliers and providers.

Successfully implemented

Your business has established a process to report and recover from data security breaches.

Your business ensures the management of data security breaches, including communication of information security events and weaknesses.

Successfully implemented

Your business has established regular information security awareness training for all staff.

Your business ensures that employees and contractors are aware of and fulfil their information security responsibilities.

Successfully implemented

Your business has established entry controls to restrict access to premises and equipment on a need-to-know basis.

Your business prevents unauthorised physical access, damage and interference to personal data.

Successfully implemented

Your business has established secure storage arrangements to protect records and equipment.

Your business prevents loss, damage, theft or compromise of personal data.

Successfully implemented

Your business has established a process to securely dispose of records and equipment when no longer required.

Successfully implemented

Your business has established a mobile working policy.

Your business ensures the security of mobile working and the use of mobile computing devices.

Successfully implemented

Your business has established a process to configure new and existing hardware to reduce vulnerabilities and provide only the functionality and services required.

Successfully implemented

Your business has established controls to manage the use of removable media.

Your business prevents unauthorised disclosure, modification, removal or destruction of personal data stored on media.

Successfully implemented

Your business has established a process to assign user accounts to authorised individuals, and to manage user accounts effectively to provide the minimum access to information.

Your business limits access to personal data held in information systems.

Successfully implemented

Your business has established appropriate password security procedures and 'rules' for information systems and has a process in place to detect any unauthorised access or anomalous use.

Successfully implemented

Your business has established effective anti-malware defences to protect computers from malware infection.

Your business ensures that personal data is protected against malware.

Successfully implemented

Your business has established a process to routinely back-up electronic information to help restore information in the event of disaster.

Your business ensures protection against the loss of personal data.

Successfully implemented

Your business has established a process to log and monitor user and system activity to identify and help prevent data breaches.

Your business records events and generates evidence.

Successfully implemented

Your business has established a process to ensure software is kept up-to-date and the latest security patches are applied.

Your business prevents the exploitation of technical vulnerabilities.

Successfully implemented

Your business has established boundary firewalls to protect computers from external attack and exploitation.

Your business ensures the protection of personal data in networks.

Successfully implemented

Your business has assigned responsibility to an appropriate member of staff for ensuring effective data sharing.

Successfully implemented

Your business provides adequate training on an ongoing basis for staff that are regularly required to make decisions regarding whether or not personal data should be shared with third parties.

Successfully implemented

Your business has agreed data sharing agreements with an appropriate legal basis with all parties with whom personal data is routinely shared or where large quantities of data are to be transferred. These agreements are regularly reviewed.

Successfully implemented

Your business informs individuals about the sharing of their personal data.

Successfully implemented

Your business has considered whether you need to provide the Information Commissioner's Office (ICO) with a description of the individuals or organisations to whom you intend or may wish to disclose personal data.

Successfully implemented

Your business has appropriate security measures in place to protect data in transit, received by your business and transferred to another business.

Successfully implemented

Your business has a documented process for processing subject access requests which has been effectively implemented.

Your business has measures in place to ensure requests are appropriately recognised, timescales are met and the appropriate information is provided.

Successfully implemented

Your business has appropriately resourced and trained all personnel assigned responsibility for processing subject access requests.

Your business has made all personnel aware of their responsibility to support subject access requests and where in the organisation they should direct requests to.

Successfully implemented

The process is monitored and reviewed and, where necessary, additional measures have been implemented to improve compliance.

Successfully implemented